Cyber Best Practices for Small Satellites

Samuel Sanders Visner and Scott Kordella
The MITRE Corporation, Fairfax, VA 22102, USA

Protection of satellites and ground systems against cyber-attack is necessary to ensure safe operations in the space sector. Protection will be required for both the command segments of and workloads served by a rapidly proliferating constellation of new, largely commercial satellites, numbering possibly in the tens of thousands. Effective and commercially viable cyber protection strategies are required that can be updated regularly to meet changing threats. Cyber protection strategies have been developed in other (non-space) sectors using collaborative processes, which has resulted in more secure systems. This paper describes some of the cyber protection work in other sectors, the collaborative processes used to develop viable cyber protection solutions, the solutions themselves that have been identified and are being used, and the lessons-learned from their use, resulting in a set of 'best-practices' in these sectors. The processes used in these domains to develop these strategies can be applied to the space domain, with similar expected results and best practices for space systems.

Keywords: cyber protection, space systems resilience

1. Introduction

Ensuring our national and economic security is urgent, especially as LEO space is exploited in new ways [1, 2]. In addition, our national interests require that we protect our nation's business and critical infrastructures. Private companies are orbiting payloads for research, communication, and manufacturing purposes that enhance economic competitiveness and security. The commercialization of LEO is creating an information technology eco-system that serves many infrastructures (communication, transportation, education); these new infrastructures will feature far more connected devices (IPv6), high-speed interconnectivity (5G wireless) and AI-mediated management of myriad resources.

As these infrastructures are introduced, their cybersecurity and resiliency will be of paramount importance. To the extent that this new information technology eco-system is supported by LEO, the US Government and commercial industry needs to ensure cybersecurity for the emerging LEO commercial participants. Industry needs effective and affordable approaches, while the U.S. government must maintain effective oversight, licensing, and regulation of these companies and set international standards for all players. Like other industries, the need to balance effective cybersecurity with other factors will assume increasing importance. For example, exquisite – but costly - measures for cyber protection could be required to allow companies to launch, but these measures might come at the expense of space commerce. What is an effective approach to ensure cybersecurity that respects the economics of small satellites and LEO?

A recently released White House Space Policy Directive (SPD5) entitled 'Cybersecurity Principals for Space Systems' [3] establishes a broad set of guidelines for space companies in developing their cyber protection approaches. These guidelines include: *(i) Protection against unauthorized access to critical space vehicle functions; (ii) Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems; (iii) Protection against communications jamming and spoofing; (iv) Protection of ground systems, operational technology, and information processing systems through the adoption of deliberate cybersecurity best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems, including from insider threats; (v) Adoption of appropriate cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements; and (vi) Management of supply chain risks that affect cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.*

To address the principals described in SPD5, a set of "resilient space best practices" guidelines should be established and made available. We envision a guidebook, developed in collaboration with government, industry, and other stakeholders, which would include straightforward approaches, such as the encryption of command/control channels between ground and satellite;

the use of design practices to segregate major subsystems onboard a satellite to reduce system-to-system coupling vulnerabilities; and separation of downlinked mission data and ground-based processors using protected interfaces. Overall, these guidelines could convey one or more "reference architectures" that show builders and operators what technologies could be brought together and implemented to strengthen cybersecurity and resilience.

These guidelines would include also the 'top N' things that must be done for a company to be allowed to fly, employing a prudent balance of cybersecurity and resiliency features. This concept has been adopted in other domains, such as wireless medical devices and threat-sharing. Real time operational coordination and use of an advanced information sharing infrastructure is being done in other critical infrastructures such as energy, transportation, and manufacturing. In this presentation, we tailor the principles used in these other applications to the LEO domain.

The discussion following is structured as follows: we identify some of the pressing threats to smallsats in LEO. We then describe analogous systems that face similar threats; namely the use by the healthcare industry of wireless infusion pumps and the threats that they face, and the approach taken to address these threats. Finally, we relate these processes to space systems.

2. Cyber Threats to Space Systems

Cyber threats to space systems attack both the satellites themselves as well as the ground systems with which they communicate. A new Space Information Sharing and Analysis Center (ISAC) [4], of which MITRE is a founding member, has been established to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member firms; and to serve as the primary communications channel for the sector with respect to this information. The Space ISAC describes threats using the following framework:

Operations Technology & Supply Chain
Concept, Design, Manufacture, Integration, Deployment, Maintenance, Retirement

Business Systems
Systems, Subsystem, Enterprise Network, Information & Communication Technology, Data Security, Software Assurance, Acquisition Planning, Commercial & Open Source Software, ERP, CRM, CMS, BI software, Training Employees, Public Contractors/Service Providers, Common Vulnerabilities & Exposures

Missions
Protected Communications, Cryptographic systems, Secure Antenna Networks, Secure Space System Architectures, RF monitoring and SSA, C2 systems, Mission Data Processing

3. National Cybersecurity Center of Excellence

The National Cybersecurity Center of Excellence (NCCoE) operates using the following Engagement & Business Model:

Design: Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble: Assemble teams of industry orgs, govt. agencies, and academic institutions to address all aspects of the cybersecurity challenge

Build: Build a practical, usable, repeatable implementation (or "reference architecture") to address the cybersecurity challenge

Advocate: Advocate adoption of the example implementation using the practice guide set of NIST Special Publications (the 1800 series)

Key tenets:

Standards-based: Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular: Develop components that can be easily substituted with alternates that offer equivalent inputoutput specifications

Repeatable: Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available: Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry; seek out innovative technologies

Usable: Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent: Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

The NCCoE addresses cyber protection needs across multiple sectors, including: Consumer retail sector, Energy sector, Finance sector, Healthcare sector, Hospitality sector, Manufacturing sector, Public Safety / First responder sector, election systems, and the Transportation sector. The portfolio of work in the NCCoE has developed a set of Cyber Security System Practice Guides (SPs) as follows:

Attribute Based Access Control (SP 1800-3)
Consumer/Retail: Multifactor Authentication for e-Commerce (SP 1800-17)
Critical Cybersecurity: Patching
Data Integrity: Identifying and Protecting
Data Integrity: Detecting and Responding
Data Integrity: Recovering (SP 1800-11)
Derived PIV Credentials (SP 1800-12)
DNS-Based Email Security (SP 1800-6)
Energy: Asset Management
Energy: Identity and Access Management (SP 1800-2)
Energy: IIoT
Energy: Situational Awareness (SP 1800-7)
Financial Services: Access Rights Management (SP 1800-9)
Financial Services: IT Asset Management (SP 1800-5)
Financial Services: Privileged Account Management (SP 1800-18)
Healthcare: Electronic Health Records on Mobile Devices (SP 1800-1)
Healthcare: Picture Archiving and Communication Systems
Healthcare: Wireless Infusion Pumps (SP 1800-8)
Healthcare: Telehealth Remote Patient Monitoring Ecosystem
Hospitality: Property Management Systems
Mitigating IoT-Based DDoS
Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems (NISTIR 8219)
Mobile Device Security: Cloud and Hybrid Builds (SP 1800-4)
Mobile Device Security: Enterprise Builds
Mobile Threat Catalogue
Privacy-Enhanced Identity Federation
Public Safety/First Responder: Mobile Application SSO (SP 1800-13)
Secure Inter-Domain Routing (SP 1800-14)
TLS Server Certificate Management (SP 1800-16)
Transportation: Maritime: Oil & Natural Gas Trusted Cloud (SP 1800 19)

4. Example: Cyber Protection in the Healthcare Sector

As an example, the NCCoE developed guidelines for securing Wireless Infusion Pumps
in Healthcare Delivery Organizations. Figure 1 depicts a basic wireless infusion pump system.

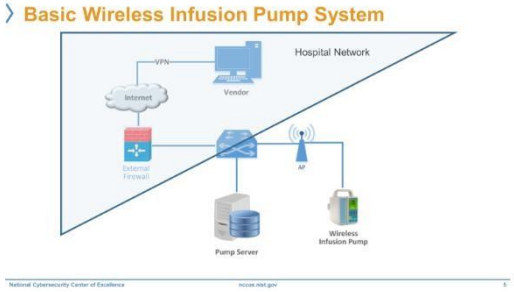

Fig. 1 Basic Wireless Infusion Pump System

The system is designed specifically for delivering medical fluid in a controllable way to a patient, using both wire and wireless networking. Many infusion pumps can be used simultaneously in the hospital systems and connected to hospital network systems. An individual pump is required to connect to a pump server for configuration setup, software update, drug library installation, etc. A small device is located with each pump, which provides limited computing. Devices communicate through various operating systems which may be fully equipped, or minimized, depending on the need. Generally, these systems are designed for relative long lifespan usage, much longer than computer technology lifecycle (such as operating systems). Like small LEOSATs, these devices are designed with an eye to functionality, rather than security. As a result, architectures using these devices require “compensating controls” in the absence of security features on-board.

Security controls for these systems include asset tracking and inventory management, patch management, remote access control, physical access control, device hardening, administrate privilege management, communication encryption, white list applications, application protection, abnormal behavior management, network segmentation and internet access control, monitoring and auditing. Figure 2. depicts security characteristics and controls for the wireless infusion pump system, and is a good example of mapping from a given process, such as risk assessment, to sector-specific standards and best practices.

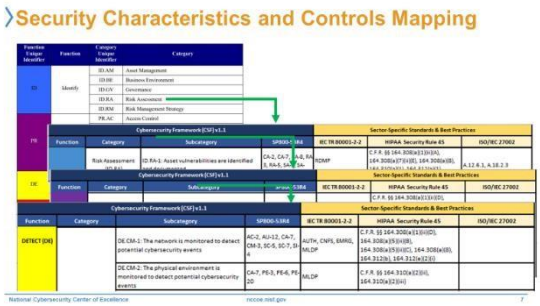

Fig. 2 Security Characteristics and Controls

Mapping

Based on this mapping the NCCoE has established a reference architecture and cybersecurity controls for wireless infusion pump systems (Figure 3) that is being adopted in the health sector. This approach has generated joint awareness within the industry of design and protection approaches which have resulted in greater security. In addition, awareness of the need for security controls has convinced some in the infusion industry to find ways to incorporate security features on-board the devices they manufacture.

Fig. 3 Reference Architecture / Cybersecurity Controls

The guidelines follow the NCCoE key tenets of being Standards-based, Modular, Repeatable, Commercially available, Usable, and Open and transparent.

5. Application of Lessons-Learned to Space Systems

The same processes developed for the medical sector can be used to address the needs of the space community, by considering a generic space architecture (Figure 4), consisting of a space segment, a ground segment and a user segment, connected by the internet.

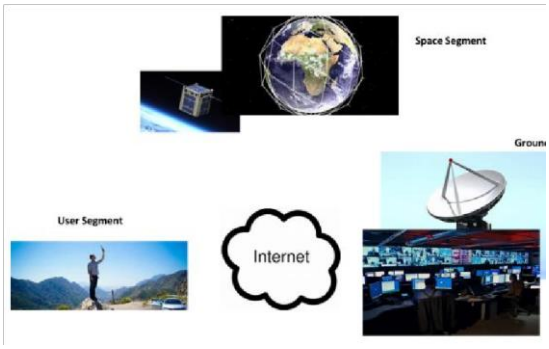

Fig. 4 Space Architecture: Space, Ground and User Segments

The space system is specially design for obtaining observations such as imagery, or communications capabilities in a controllable way to a patient, using distributed ground/satellite networking. Many satellites can be used simultaneously in a given system and connected to multiple ground network systems.

An individual satellite is required to connect to a satellite data server for configuration setup, software update, collection, and operating instruction library installation, etc. On board computers, located with each satellite, provide limited computing. Satellites communicate through various operating systems which may be fully equipped, or minimized, depending on the need. In the case of space systems, systems are designed for relative short lifespan usage to enable de-orbit and replenishment.

Drawing the analogy to other NCCoE supported sectors, we believe that the same approach should be applied to the space sector. Based on our experience in numerous other sectors, we anticipate that a set of bestpractices for smallsat systems will contain these elements: 1) Authenticated Communication; 2) Encryption of Data in Transmit; 3) Access Control; 3) White Listing and Input Verification/Constraints; 4) Logging and Auditing; 5) Secure Updates; 6) Secure Engineering Processes; 7) Antivirus Capabilities; 8) BIOS Security and 9) Fail Safe Capability

6. Summary

The approach used by the National Cybersecurity Center of Excellence and MITRE might well be a useful guide to developing reference architectures to be used by the proliferating population of LEOSATs. These architectures are not mandatory, but their adoption can be regarded as "best practices" that savvy operators will employ, and on which their customers and users might well insist. The collaborative approach, which brings tighter resources from industry, government, and academia, representing both users and product manufacturers, results in both effective and practice cybersecurity architectures and, as in the case of the wireless infusion pump industry, encouragement to improve security of specific devices, apart from the architecture. Such an approach might be an effective model of government/industry collaboration as these new satellites are prepared for launch.

References

[1] National Cyber Strategy of the United States, September 2018

[2] National Space Policy Directive-3, National Space Traffic Management Policy, June 18, 2018

[3] National Space Policy Directive-5, Cybersecurity Principles for Space Systems, September 5, 2020
[4] Space Information Sharing and Analysis Center (ISAC)
[5] National Institute of Standards and Technology Cyber Center of Excellence (NCCoE)